International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

Secret Communication with Feedback

Deniz Gündüz[†‡], D. Richard Brown III[††] and H. Vincent Poor[†]

[†] Dept. of Electrical Engineering, Princeton University, Princeton, NJ, 08544.
[‡] Dept. of Electrical Engineering, Stanford University, Stanford, CA, 94305.
[††] Dept. of Electrical and Computer Eng., Worcester Polytechnic Institute, Worcester, MA, 01609.

arXiv:0812.1713v1 [cs.IT] 9 Dec 2008

Abstract

Secure communication with feedback is studied. An achievability scheme in which the backward channel is used to generate a shared secret key is proposed. The scenario of binary symmetric forward and backward channels is considered, and a combination of the proposed scheme and Maurer's coding scheme is shown to achieve improved secrecy rates. The scenario of a Gaussian channel with perfect output feedback is also analyzed and the Schalkwijk-Kailath coding scheme is shown to achieve the secrecy capacity for this channel.

1. Introduction

In his pioneering work [1], Shannon introduced information theoretic security and defined perfect secrecy, which roughly refers to the case in which an enciphered cryptogram does not reveal any information to an eavesdropper about the underlying secret message. Shannon proved that perfect secrecy can be achieved with a shared secure key that is as long as the underlying message. Wyner showed in [2] that perfect secrecy can be achieved even without key distribution if the cryptogram is transmitted over a noisy broadcast channel in which the eavesdropper's channel is physically degraded with respect to the legitimate receiver's channel. This result was extended to more general broadcast channels in [3], where it was shown that nonzero secrecy capacity can be achieved if the main channel is *less noisy* than the eavesdropper's channel. Secure communication in the presence of eavesdroppers has gained a recent interest, and information theoretic security in various models has been explored in detail (see, for example, [4], [5], [6] and [7]).

While it is well-known that feedback doesn't increase the capacity of a point-to-point memoryless channel, it was observed in [8] that the availability of feedback might increase the *secrecy capacity* of a point-to-point memoryless channel. This can be immediately seen by considering an infinite capacity secure feedback link from the legitimate receiver to the legitimate transmitter. The feedback link can be used to transmit a secure key. This secure key can then be used to transmit the message securely over the forward channel via the one-time-pad coding scheme. Hence, an infinite capacity secure feedback channel allows the system to achieve a secrecy capacity equal to the forward channel capacity as if the eavesdropper is not present. It is observed in [9], [10] that even public communication between the legitimate users can enhance the secrecy capacity. It has been shown that positive secrecy capacity can be achieved through public communication even if the eavesdropper's forward channel is *less noisy*. In [9] and [10] upper and lower bounds for the perfect secrecy capacity are provided in the case of public communication. These bounds match only for certain special cases. A feedback jamming scheme is also described in [11] for modulo additive channels.

In this paper, we first propose an achievable secrecy scheme for a general wiretap channel model with feedback (see Fig. 1), in which the forward channel from Alice to Bob and Eve and the backward channel from Bob to Alice and Eve are orthogonal broadcast channels. The achievability of the proposed scheme follows from using the backward channel for generating a secret key shared by Alice and Bob and then using this secret key to transmit the message securely over the forward channel via the one-time-pad coding scheme. We then apply this secrecy scheme, in conjunction with Maurer's feedback coding technique [9], to a scenario with independent binary symmetric forward and backward channels. We explicitly describe the achievable secrecy rates of the proposed scheme and show the improvements in secrecy rate achieved with respect he feedback scheme for binary symmetric channels proposed in [12].

In the second part of this paper, we consider secret communication through a Gaussian wiretap channel with perfect channel output feedback, i.e., Bob's

This research was supported by the US National Science Foundation under grants CCF-04-47743, ANI-03-38807, and CNS-06-25637.

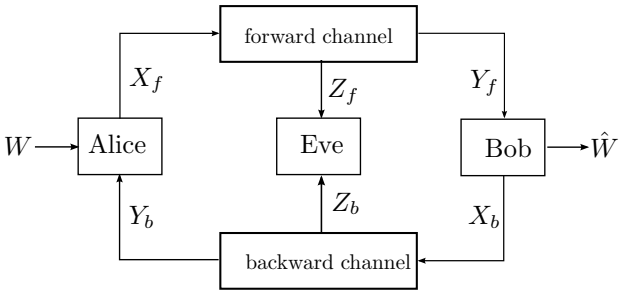

Figure 1: Wiretap channel with noisy feedback channel whose output can also be observed by the eavesdropper.

noisy channel output is perfectly available to Alice in a casual manner. This system is consistent with the model considered in the Schalkwijk-Kailath (SK) [13] scheme, where perfect causal feedback was shown to greatly simplify the achievability of the point-to-point link from Alice to Bob and also improve the error exponent by exploiting the perfect feedback link in this scenario. The SK scheme is a simple deterministic scheme which is easy to implement and analyze as opposed to Shannon theoretic random coding involving long codewords and high complexity encoding/decoding. We show that, in addition to all these attractive properties, the SK scheme also achieves the secrecy capacity in the presence of an eavesdropper when the eavesdropper (Eve) receives a noisy observation of the feedback from Bob in addition to her own channel output from Alice as depicted in Fig. 4.

In the rest of the paper, we use X^n and X_i^n to denote the sequences $(X_1, \ldots, X_n)$ and $(X_i, \ldots, X_n)$, respectively. We also define $[x]^+ = \max\{x, 0\}$.

2. System Model and Definitions

In the system shown in Fig. 1, Alice wants to transmit a message $W \in \mathcal{W}$ to Bob over the discrete memoryless broadcast channel $p(y_f, z_f|x_f)$, where $X_f \in \mathcal{X}_f$ is Alice's channel input and $Y_f \in \mathcal{Y}_f$ and $Z_f \in \mathcal{Z}_f$ are the outputs at Bob and Eve, respectively. There is also an independent feedback channel $p(y_b, z_b|x_b)$, where $X_b \in \mathcal{X}_b$ is Bob's feedback channel input and $Y_b \in \mathcal{Y}_b$ and $Z_b \in \mathcal{Z}_b$ are the outputs at Alice and Eve, respectively. Here, subscripts 'f' and 'b' represent *forward* and *backward* channels, respectively.

Definition 2.1 *A $(2^{nR}, n)$ code for the above feedback channel is composed of a message W uniformly distributed over set $\mathcal{W} = \{1, \ldots, 2^{nR}\}$, stochastic encoders at Alice $f_i : \mathcal{W} \times \mathcal{Y}_b^{i-1} \to \mathcal{X}_f$ which map the message and the previous feedback outputs to the i-th channel input, and stochastic feedback encoders at Bob $g_i : \mathcal{Y}_f^{i-1} \times \mathcal{X}_b^{i-1} \to \mathcal{X}_b$ which map previous channel outputs and the feedback inputs to the i-th feedback input, $i = 1, \ldots, n$, and finally a decoder at Bob $h : \mathcal{Y}_f^n \times \mathcal{X}_b^n \to \mathcal{W}$, which maps the channel outputs and the feedback inputs of Bob to the decoded message $\hat{W}$.*

As usual, the block error probability of a code is defined as

$$P_e^n = \frac{1}{2^{nR}} \sum_{W=1}^{2^{nR}} \Pr\{\hat{W} \neq W\}, \tag{1}$$

while the equivocation rate is defined as

$$R_e^n = \frac{1}{n} H(W|Z_f^n, Z_b^n). \tag{2}$$

Definition 2.2 *A secrecy rate R is achievable if there exists a sequence of $(2^{nR}, n)$ codes for which $P_e^n \to 0$ as n goes to infinity and the equivocation rate satisfies*

$$R \leq \lim_{n\to\infty} R_e^n.$$

Definition 2.3 *The* secrecy capacity $\mathcal{C}_{sf}$ *in the presence of feedback is the highest achievable rate R.*

3. An Achievable Secrecy Rate

In the following theorem, we give a lower bound to the secrecy capacity in the presence of feedback. The achievability follows from using the backward channel for generating a secret key shared by Alice and Bob, and then using this secret key in the forward channel to increase the secrecy capacity of the forward channel.

Theorem 3.1 *Rate R_s is achievable if,*

$$0 \leq R_s \leq \min\{I(V_f; Y_f), I(V_f; Y_f|U_f) - I(V_f; Z_f|U_f) + I(V_b; Y_b) - I(V_b; Z_b)\},$$

for some auxiliary random variables U_f, V_f, and V_b satisfying $I(U_f; Z_f) \geq I(U_f; Y_f)$ with a joint distribution $p(v_b, x_b, y_b, z_b, u_f, v_f, x_f, y_f, z_f) = p(v_b) \cdot p(x_b|v_b)p(y_b, z_b|x_b)p(u_f)p(v_f|u_f)p(x_f|v_f)p(y_f, z_f|x_f)$, i.e., $U_f \to V_f \to X_f \to (Y_f, Z_f)$ and $V_b \to X_b \to (Y_b, Z_b)$.

Proof: The achievability scheme is based on a separation approach in the sense that, Bob uses the backward channel to generate a shared secret key of rate R_k, and then this shared key is used to transmit the message W over the direct channel. We can utilize a block based coding structure, where a secure key is generated in the i-th block, $i = 1, \ldots, B$, and used in block

$i+1$, and the desired rate is achieved in the limit of infinite blocks, i.e., as $B \to \infty$.

For simplicity, we give the proof for a constant U_f. Also, for given $P_{V_f X_f Y_f Z_f}$, one can consider an auxiliary channel $P_{X_f|V_f}$ and the code for the induced channel $P_{Y_f Z_f|V_f} = \sum_{x_f} P_{X_f|V_f}(x_f|v_f) P_{Y_f Z_f|X_f}(y_f, z_f|x_f)$. Hence, we prove the achievability of $\min\{I(X_f;Y_f), I(X_f;Y_f) - I(X_f;Z_f) + I(V_b;Y_b) - I(V_b;Z_b)\}$. The more general proof follows as in [3]. It is possible to generate a secret key W_k at rate

$$R_k \triangleq \min\{[I(V_b;Y_b) - I(V_b;Z_b)]^+, I(X_f;Z_f)\}.$$

over the backward channel [3]. From the perspective of the forward channel, the problem is now equivalent to finding the secrecy capacity of the broadcast channel with a secret key of rate R_k.

Let $R_1 \triangleq I(X_f;Y_f) - I(X_f;Z_f)$. Generate $2^{nI(X_f;Y_f)}$ codewords independent identically distributed (i.i.d.) with probability $p(x_f^n) = \prod_{i=1}^n p(x_{fi})$, and partition these codewords into 2^{nR_1} codebooks which we name as $\mathcal{C}_1, \ldots, \mathcal{C}_{2^{nR_1}}$. Further divide each subcodebook $\mathcal{C}_i$ into 2^{nR_k} smaller codebooks, which are named as $\mathcal{C}_{i,1}, \ldots, \mathcal{C}_{i,2^{nR_k}}$. For each message $w = [w_1, w_2]$, where $w_1 \in [1, 2^{nR_1}]$ and $w_2 \in [1, 2^{nR_k}]$, first generate $w_2' = w_2 \oplus w_k \mod(2^{nR_k})$, and transmit a codeword chosen uniformly random from the codebook $C_{w_1,w_2'}$. Bob can correctly find (w_1, w_2'), hence w_1 using the secret key, with high probability for large enough n. On the other hand, Eve can determine w_2' and the codeword index within the smallest codebook, but cannot receive any information about w_1. Moreover, no information about w_2 is revealed to Eve as well, because w_2' is uniformly distributed and independent of w_2.

Corollary 3.2 *If Bob's channel in the forward direction and Alice's channel in the backward direction are both less noisy then Eve's, the highest secrecy rate achievable by the proposed scheme in Theorem 3.1 can be simplified as*

$$\begin{aligned} R_s \quad \leq \quad & \min\{I(X_f;Y_f), I(X_f;Y_f) - I(X_f;Z_f) \\ & + I(X_b;Y_b) - I(X_b;Z_b)\}, \end{aligned}$$

for a joint distribution of the form $p(x_b)\ p(y_b, z_b|x_b)\ p(x_f)\ p(y_f, z_f|x_f)$.

4. Secrecy Rates for the Binary Symmetric Wiretap Channel with Feedback

In this section, we focus on the secrecy rates when both the forward and the backward channels in Fig. 1 are independent binary symmetric channels (BSCs). The system model in this case is fully characterized by the four crossover probabilities ϵ_f, δ_f, ϵ_b, and δ_b, corresponding to the channels Alice→Bob, Alice→Eve, Bob→Alice, and Bob→Eve, respectively.

This model is also analyzed in [12] in which a secrecy rate based on the transmission scheme proposed by Maurer in [9] is proposed: a random binary sequence x_b^n is transmitted by Bob over the backward channel. Assuming Alice's coded message is v^n, she transmits the modulo sum of v^n with the received signal from the backward channel, i.e., $x_f^n = v^n \oplus y_b^n$. If we assume that Alice can transmit x_f^n over a noiseless channel, then Bob can reconstruct $v^n \oplus y_b^n \oplus x_b^n$, while the best Eve can do is to reconstruct $v^n \oplus y_b^n \oplus z_b^n$. This is equivalent to a broadcast channel from Alice to Bob and Eve with cross-over probabilities ϵ_b and $\epsilon_b + \delta_b - 2\epsilon_b\delta_b$, respectively.

We propose here to use a combination of Maurer's scheme with the proposed scheme in Section 3. The maximum secret key rate that can be generated using the feedback channel is $C_s^b \triangleq [h(\delta_b) - h(\epsilon_b)]^+$. Bob uses the first αn channel uses to generate a secret key of rate αC_s^b, where $0 \leq \alpha \leq 1$ is a design parameter that can be optimized according to the crossover probabilities in order to maximize the total secrecy rate. Bob transmits random bits in the rest of the feedback channel uses.

In the forward channel, we first consider the case $\epsilon_f < \delta_f$. Alice divides the secret message into three parts, all of which are transmitted simultaneously. In the first part, Alice transmits a secret message of rate

$$R_1^s = h(\delta_f) - h(\epsilon_f)$$

over the forward channel using the usual secret coding scheme. Alice can simultaneously transmit a message at rate $1 - h(\epsilon_f) - R_1^s = 1 - h(\delta_f)$, which can be received by both Bob and Eve. Alice uses the secure key from the feedback channel as a one-time-pad to transmit securely to Bob at rate

$$R_2^s = \min\{1 - h(\delta_f), \alpha C_s^b\}.$$

The remaining capacity of the forward channel is then $1 - h(\delta_f) - R_2^s = [1 - h(\delta_f) - \alpha C_s^b]^+$. Finally, at this rate, Alice transmits a modulo summed message in the same manner as [12], using the random bits received from the second portion of the feedback channel. This transmission occurs at rate

$$\begin{aligned} R_3^s = \quad & \min\Big\{[1 - h(\delta_f) - \alpha C_s^b]^+, (1-\alpha)\Big\} \\ & \cdot (h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b)) \end{aligned}$$

In the case when $\epsilon_f \geq \delta_f$, it is impossible to have secret communication without feedback, hence $R_1^s = 0$. It is

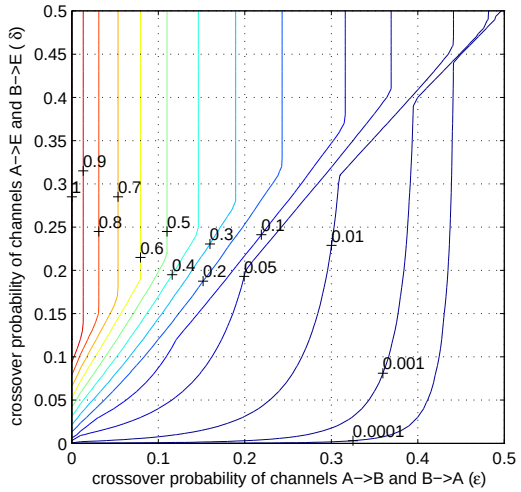

Figure 2: Achievable secrecy rate of the proposed feedback scheme with optimized α in binary symmetric channels.

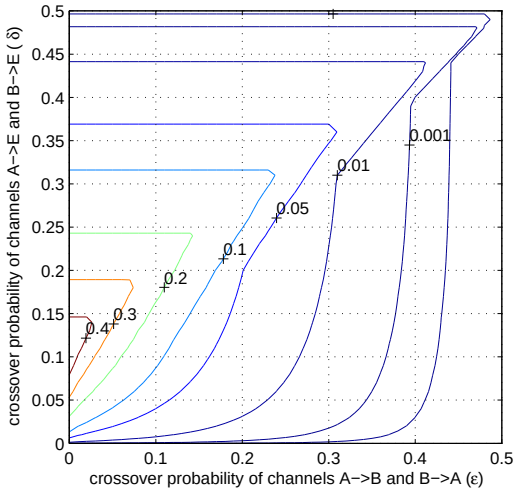

Figure 3: Improvement in secrecy rate of the proposed feedback scheme with optimized α in binary symmetric channels with respect to secrecy capacity without feedback.

straightforward to show in this case that $R_2^s = \min\{1 - h(\epsilon_f), \alpha C_s^b\}$ and $R_3^s = \min\{[1 - h(\epsilon_f) - \alpha C_s^b]^+, (1-\alpha)\}(h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b))$. In both cases, the total secrecy capacity is then $R_1^s + R_2^s + R_3^s$.

To illustrate the gains through the proposed feedback technique, we consider a system model with the same crossover probability in the forward and backward channels, i.e. $\epsilon = \epsilon_f = \epsilon_b$ and $\delta = \delta_f = \delta_b$. In Fig. 2, we plot the achievable secrecy rate by the proposed transmission scheme with optimized α as a function of ϵ and δ. As opposed to not having feedback, or using the whole feedback link to generate a secret key, this scheme can achieve positive secrecy rates even in $\delta > \epsilon$ as we have partially incorporated Maurer's coding scheme. Note also that, our achievable secrecy rates improve upon the ones reported in [12].

Figure 3 plots the improvement in the secrecy rate of the proposed feedback scheme with respect to the secrecy capacity without feedback. Note that the secrecy capacity without feedback is $C_s = [h(\delta) - h(\epsilon)]^+$. Interestingly, the largest gain is obtained at the point $\epsilon = 0$ and $h(\delta) = \frac{1}{2}$, or $\delta \approx 0.11$. At this point the secrecy rate without feedback is $C_s = \frac{1}{2}$, while with feedback we achieve $C_{sf} = 1$, an improvement of one half bit. As $\delta \to \frac{1}{2}$ from this point, the secrecy capacity without feedback increases towards one and feedback results in less improvement.

5. Gaussian Wiretap Channel with Perfect Feedback

Here, we consider a Gaussian wire-tap channel with feedback as seen in Fig. 4. The forward channel at time index i is modeled as

$$Y_i = X_i + N_i \text{ and } Z_i = X_i + M_i,$$

in which N_i and M_i are additive white jointly Gaussian noise terms with zero means. There is also an average power constraint P on Alice's transmission. We also have a perfect feedback channel from Bob's output to Alice that operates causally, i.e., at time instant i, Alice knows Bob's previous channel outputs $Y^{i-1} = \{Y_1, \ldots, Y_{i-1}\}$. Eve, on the other hand, can only observe a noisy version of this feedback. The feedback from Bob to Alice, as overheard by Eve, is modeled as

$$\bar{Y}_i = Y_i + S_i, \tag{3}$$

at time i, where S_i is also white Gaussian with zero mean. We allow correlation among the additive noise terms of the network at each time instant. The covariance matrix of the noise terms N, M and S is defined as

$$\mathbf{C} \triangleq \begin{bmatrix} \sigma_N^2 & \rho_1\sigma_N\sigma_M & \rho_2\sigma_N\sigma_S \\ \rho_1\sigma_N\sigma_M & \sigma_M^2 & \rho_3\sigma_M\sigma_S \\ \rho_2\sigma_N\sigma_S & \rho_3\sigma_M\sigma_S & \sigma_S^2 \end{bmatrix}$$

which is a real, non-negative definite matrix with $\sigma_M^2 > 0$, $\sigma_S^2 > 0$ and $|\rho_i| < 1$, for $i = 1, 2, 3$.

Alice's (potentially stochastic) encoding functions are now defined as $f_i : \mathcal{W} \times \mathcal{Y}^{i-1} \to \mathcal{X}$. We do not have

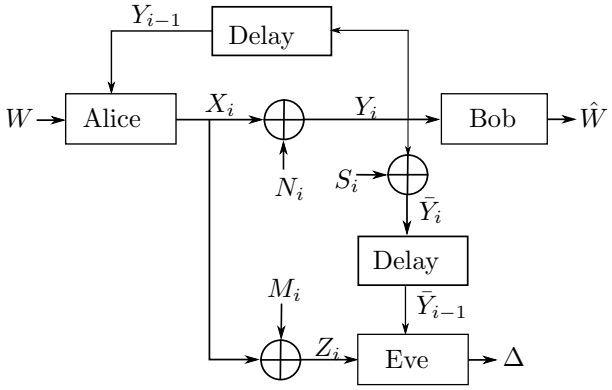

Figure 4: The Gaussian wiretap channel with perfect feedback to the legitimate transmitter.

a channel encoder at Bob, and the perfect feedback scenario is equivalent to having $X_{b,i} = Y_{b,i} = Y_i$ and $Z_{b,i} = \bar{Y}_i$. The average probability of error and the equivocation rate are as defined in Section 2.

Ignoring the eavesdropper, the capacity from Alice to Bob (with or without feedback) is $\mathcal{C}_f = \frac{1}{2}\log\left(1+\frac{P}{\sigma_N^2}\right)$. This also serves as an upper bound on the secrecy capacity with feedback. The secrecy capacity when there is no feedback is given by [8]

$$\mathcal{C}_s = \frac{1}{2}\left[\log\left(1+\frac{P}{\sigma_N^2}\right) - \log\left(1+\frac{P}{\sigma_M^2}\right)\right]^+. \qquad (4)$$

Note that $\mathcal{C}_s = 0$ if $\sigma_N^2 \geq \sigma_M^2$.

In [13], Schalkwijk and Kailath proposed a communication scheme (the SK scheme) for a Gaussian channel with perfect feedback that achieves the channel capacity. The SK scheme is based on deterministic coding and parameter estimation. We first give a brief overview of the SK scheme using the notation of [14].

In the SK scheme, 2^{nR} messages are mapped to a signal point by dividing the interval $[-0.5, 0.5]$ into 2^{nR} equally spaced subintervals. The mid-point of each subinterval corresponds to a message. Let θ be the signal point corresponding to the underlying message. At the first transmission, $X_1 = \alpha_1\theta$ is transmitted, and $Y_1 = \alpha_1\theta + N_1$ is received where α_1 is a constant to be chosen. The receiver forms an estimate of θ based on its observation as

$$\hat{\theta}_1 = \hat{X}_1 = \frac{Y_1}{\alpha_1} = \theta + \frac{N_1}{\alpha_1}. \qquad (5)$$

The transmitter can also compute this estimate using the perfect feedback signal, and in the next transmission, it transmits the estimation error at the receiver, i.e., $X_2 = \alpha_2(\theta - \hat{\theta}_1) = -\alpha_2\frac{N_1}{\alpha_1}$, where α_2 is another pre-determined constant. The receiver computes

$$\hat{X}_2 = \frac{Y_2}{\alpha_2} + \frac{Y_1}{\alpha_1} = \theta + \frac{N_2}{\alpha_2}. \qquad (6)$$

Using the two independent observations of θ in (5) and (6), the receiver forms $\hat{\theta}_2$ the maximum likelihood (ML) estimate of θ. Then the transmitter transmits $X_3 = \alpha_3(\theta - \hat{\theta}_2)$, where α_3 is another pre-determined constant. Repeating this process, we have

$$X_i = \alpha_i(\theta - \hat{\theta}_{i-1}), \qquad (7)$$

$$\hat{X}_i = \hat{\theta}_{i-1} + \frac{Y_i}{\alpha_i}, \text{ and} \qquad (8)$$

$$\hat{\theta}_i = \frac{\sum_{j=1}^{i}\alpha_j^2\hat{X}_j}{\sum_{j=1}^{i}\alpha_j^2} \qquad (9)$$

where (9) is the maximum likelihood (ML) estimate of the parameter θ at Bob from the observations $Y[1], \ldots, Y[i]$.

Now, on choosing $\alpha_i = \gamma\alpha^{i-1}$ with $\gamma = \sqrt{P/\sigma_N^2}$ and $\alpha_1 = \alpha = \sqrt{\frac{P+\sigma_N^2}{\sigma_N^2}}$, it can be shown that the error variance after n iterations is $E[(\theta - \hat{\theta}_n)^2] = \frac{\sigma_N^2}{\alpha^{2n}}$. For $M = 2^{nR}$, the probability of error, which corresponds to the probability of $\hat{\theta}_n$ falling outside of the message interval, can be shown to decay to zero exponentially.

In the following theorem, we show that the SK scheme also achieves the optimal secrecy capacity.

Theorem 5.1 *For the additive white Gaussian noise (AWGN) wire-tap channel with perfect feedback to the transmitter, the secrecy capacity is given by*

$$\mathcal{C}_{sf} = \mathcal{C}_f = \frac{1}{2}\log\left(1+\frac{P}{\sigma_N^2}\right), \qquad (10)$$

and this capacity can be achieved by the SK scheme.

Proof: The converse is obvious since the rate in (10) is the capacity of the feedback channel without secrecy constraints. Here we prove the achievability of the secrecy capacity in (10) by the SK scheme.

Fix $\mathcal{W} = \{1, \ldots, 2^{nR}\}$, where $R = \mathcal{C}_{sf} - \epsilon$, for some $\epsilon > 0$. Then we know that the average error probability goes to zero as $n \to \infty$ for any $\epsilon > 0$ with the SK scheme.

From the SK scheme, we can observe that

$$\hat{\theta}_i = \theta + \frac{\sum_{j=1}^{i}\alpha_j N_j}{\sum_{j=1}^{i}\alpha_j^2}, \text{ and} \qquad (11)$$

$$X_i = -\alpha_i\frac{\sum_{j=1}^{i-1}\alpha_j N_j}{\sum_{j=1}^{i-1}\alpha_j^2} = h_i\sum_{j=1}^{i-1}\alpha_j N_j \qquad (12)$$

where we have defined $h_i \triangleq -\frac{\alpha_i}{\sum_{j=1}^{i-1}\alpha_j^2}$. The observations at Eve are then given as $Z_1 = \alpha_1\theta + M_1$ and

$$Z_i = \alpha_i \sum_{j=1}^{i-1} h_j N_j + M_i, \text{ for } i = 2, \ldots, n. \tag{13}$$

Finally, the equivocation rate can be written as

$$\begin{aligned} H(\theta|Z_1^n,\bar{Y}_1^n) &\geq H(\theta|Z_1^n,\bar{Y}_1^n,M_2^n), &(14)\\ &= H(\theta|\alpha_1\theta+M_1,\alpha_1\theta+S_1,S_2^n,N^n,M_2^n),\\ &= H(\theta|\alpha_1\theta+M_1,\alpha_1\theta+S_1,N_1), &(15)\end{aligned}$$

where (14) follows from the fact that conditioning reduces entropy and (15) follows since N_2^n and M_2^n are independent of both θ and $\alpha_1\theta + M_1$ due to i.i.d. channel assumption.

The equivocation rate can be further simplified as

$$\begin{aligned} H(\theta|Z_1^n,\bar{Y}_1^n) &\geq H(\theta|\alpha_1\theta+M_1,\alpha_1\theta+S_1,N_1),\\ &= H(\theta) - I(\theta;\alpha_1\theta+M_1,\alpha_1\theta+S_1,N_1),\\ &= nR - I(\theta;\alpha_1\theta+M_1,\alpha_1\theta+S_1,N_1),\\ &= nR - I(\theta;\mathbf{A}\theta+\mathbf{B}),\end{aligned}$$

where $\mathbf{A} \triangleq [0,\alpha_1,\alpha_1]^T$, $\mathbf{B} \triangleq [N_1,M_1,S_1]^T$, and where we have used the fact that the message is uniform over the set $\{1,\ldots,2^{nR}\}$. The mutual information term in the final expression is difficult to calculate for a uniformly distributed discrete θ, but we know that, allowing for an arbitrary distribution for θ, the mutual information is maximized for a Gaussian input distribution that has the same variance as θ. The variance of θ as n goes to infinity is $\frac{1}{12}$, hence the corresponding mutual information upper bound is given by

$$\begin{aligned} I(\theta;\mathbf{A}\theta+\mathbf{B}) &\leq \frac{1}{2}\log\det\left(\mathbf{I}+\frac{1}{12}\mathbf{A}\mathbf{A}^T\mathrm{E}[\mathbf{B}\mathbf{B}^T]^{-1}\right)\\ &= \frac{1}{2}\log\det\left(\mathbf{I}+\frac{1}{12}\mathbf{A}\mathbf{A}^T\mathbf{C}^{-1}\right)\\ &= \frac{1}{2}\log\left(1+\frac{\alpha_1^2c_1}{12\sigma_S^2\sigma_M^2c_2}\right) &(16)\end{aligned}$$

where

$c_1 \triangleq 2(\rho_3-\rho_1\rho_2)\sigma_S\sigma_M + (\rho_1^2-1)\sigma_M^2 + (\rho_3^2-1)\sigma_S^2$ and $c_2 \triangleq \rho_1^2+\rho_2^2+\rho_3^2-2\rho_1\rho_2\rho_3-1$.

Overall, we obtain

$$\begin{aligned} \frac{1}{n}H(\theta|Z_1^n,\bar{Y}_1^n) &\geq R - \frac{1}{2n}\log\left(1+\frac{\alpha_1^2c_1}{12c_2\sigma_S^2\sigma_M^2}\right)\\ &= \mathcal{C}_{sf} - \epsilon - \frac{1}{2n}\log\left(1+\frac{\alpha_1^2c_1}{12c_2\sigma_S^2\sigma_M^2}\right)\\ &\to \mathcal{C}_s^f &(17)\end{aligned}$$

as $n\to\infty$ and $\epsilon\to 0$, if $\sigma_M^2>0$, $\sigma_S^2>0$ and $c_2\neq 0$.

Note that, when there is no feedback, the secrecy capacity is nonzero only if $\sigma_N^2 < \sigma_M^2$. However, our result shows that even if the eavesdropper's channel is less noisy than that of the legitimate receiver, the secrecy capacity can be made positive via perfect feedback.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[5] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, submitted.

[7] D. Gündüz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Inf. Theory Workshop*, Porto, Portugal, May 2008.

[8] S. K. Leung-Yan-Cheong, *Multi-user and Wiretap Channels Including Feedback*. Stanford Univ.: Ph.D. thesis, Dept. of Electrical Engineering, July 1976.

[9] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[10] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[11] L. Lai, H. El-Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, to appear.

[12] G. T. Amariucai and S. Wei, "Strictly positive secrecy rates of binary wiretapper channels using feedback schemes," in *Proc. Conf. on Inf. Sciences and Systems (CISS)*, Princeton, NJ, March 2008.

[13] J. P. M. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback. part I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, pp. 172–182, Apr. 1966.

[14] S. R. B. Pillai, *Broadcast, Relay and Feedback in Gaussian Channels*. EPFL: Ph.D. Thesis, Information Theory Laboratory (LTHI), 2007.